UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/520,251	07/27/2005	Klaus Huber	2345/206	2614

26646 7590 04/01/2009

KENYON & KENYON LLP
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
MEHEDI, MORSHED D	
ART UNIT	PAPER NUMBER
4124	
MAIL DATE	DELIVERY MODE
04/01/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/520,251	HUBER ET AL.	
	Examiner	Art Unit	
	MORSHED MEHEDI	4124	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *13-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *13-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *08/22/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for foreign priority under 35 U.S.C. 119(e) is acknowledged.

2. The application is filed on 07/27/2005 but claims the benefit of 371 application number PCT/DE03/01917 filed on June 11, 2003, which claims the benefit of foreign application number 102 29 811.4 filed on July 3rd 2002. Therefore, the effective filing date for the subject matter defined in the pending claims in this application is 07/03/2002.

Specification

1. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: the specification lacks written description of “data carrier” to enable one of ordinary skill of art to determine what constitute a data carrier.

Claim Objections

2. **Claim 16** is objected to because of the following informalities: unclear symbol between 'k' and 'm' in line 1 and line 2.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. **Claim 16** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. **Claim 16** recites the limitation "the constants" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 13-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 13-21 are non-statutory because the claims recite a process without the method steps tied to a machine.

Claim 22 recites software per se and is non-statutory.

Claim 23 recite a data carrier (carrier wave). Such subject matter is a natural phenomena and is as non-statutory.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 13-17 and 20-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Etzel et al. (US Patent No. 6,266,411 B1) in view of Brands (US Patent No. 6,052,467) further in view of Cocks ("An Identity Based Encryption Scheme Based on Quadratic Residues").

Regarding claim 13, Etzel does disclose in column (2 lines 31-56) that the first input transformed message is processed by a first iteration of a CMEA process using the first CMEA key to produce a first intermediate cipher text. This first intermediate cipher text is subjected to a first output transformation to produce a first output transformed message. The first output transformed message is subjected to a second input transformation to produce a second input transformed message. The second input transformed message is processed by a second iteration of the CMEA process using the second CMEA key to produce a second intermediate cipher text. The second intermediate cipher text is subjected to a second output transformation to produce a second output transformed message. According to another aspect of the present invention, the first and second iterations of the CMEA process employ tbox functions with inputs permuted by secret offsets. According to another aspect of the present invention, the plaintext may be processed by first and second iterations of the CMEA process using first and second CMEA keys, without being subjected to input and output transformations. Encrypted text may be suitably decrypted by introducing cipher text and reversing in order and inverting the steps applied to encrypt plaintext.

Etzel does not explicitly disclose regarding defining keys (public and private) and message decryption utilizing quadratic equation.

However, Brands does disclose in column (7 lines 1-5) that the composite number n is a product of two distinct prime numbers p and q. The secret key is the prime factorization of n where the secret key is private key.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Etzel to include factorized private key for the advantage of providing greater protection against attacks on data transmission.

Etzel and Brands are cited the claim limitation above. However, the combination of Etzel and Brands fails to specifically disclose regarding elements of public key and message decryption utilizing quadratic equation.

However, Cocks does disclose in page (360 sections 2) that the system generates a universally available public modulus M. This modulus is a product of two primes P and Q where the modulus M is a public key. Cocks does disclose in page (361 section 3 lines 7-32) that a is a square modulo both P and Q, and hence is a square modulo M, or else –a is a square modulo P, Q and hence M. either a or –a will be quadratic residues modulo P and Q where the authority can calculate the square root modulo M and send it to Alice. Alice decrypted message s by calculating Jacobi symbol to recover original message.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Etzel and Brands to include quadratic equation for message decryption for the advantage of preventing attacks by providing greater protection on encrypted data transmission.

Regarding claim 14, in reference to claim 13, Cocks does disclose in page (362 lines 7-11) that for a 128 bit transport key, and using a 1024 bit modulus M, Bob will need to send 16K bytes of keying material. If Bob does not know whether

Alice has received the square root of a or of − a then he will have to transmit

double where Alice received additional bits to eliminate multiple values of a in order to recover original message.

Regarding claim 15, in reference to claim 13, Cocks does disclose in page (360 sections 2) that this modulus is a product of two primes P and Q - held privately by the authority, where P and Q are both congruent to 3 mod 4. Cocks does disclose in page (361 lines 28-32) that Alice recovers the bit x, by calculate the Jacobi symbol by using the value r, encrypted message s and modulo M where M is a composite number of prime numbers p and q.

Regarding claim 16, in reference to claim 13, Etzel does disclose in figure (3) and column (4 lines 60-66) that at step 306, the first input transformed message is subjected to a first iteration of a CMEA process using a first CMEA key to produce a first intermediate cipher text. Etzel does disclose in figure (3) and column (5 lines 9-15) that at step 312, the transformed intermediate cipher text is subjected to a second iteration of the CMEA process, using a second CMEA key to produce a second intermediate cipher text. The second iteration of the CMEA process preferably employs the improved use of the tbox function described in our above mentioned application.

Regarding claim 17, in reference to claim 13, Cocks does disclose in page (360 sections 2) that the system generates a universally available public modulus M. This modulus is a product of two primes P and Q where the modulus M is a public key where prime numbers P and Q are both congruent to 3 mod 4.

Regarding claim 20, in reference to claim 13, Cocks does disclose in page (361 lines 33-36) that if Bob does not know which of a or − a is the square for which Alice holds the root, he will have to replicate the above, using different randomly chosen t values to send the same x bits as before, and transmitting s = (t − a/t) mod M to Alice at each step. This doubles the amount of keying data that Bob sends where multiple values of a is resolved by transmitting additional data from Bob to Alice.

Regarding claims 21-24, Etzel does disclose in column (2 lines 31-56) that the first input transformed message is processed by a first iteration of a CMEA process using the first CMEA key to produce a first intermediate cipher text. This first intermediate cipher text is subjected to a first output transformation to produce a first output transformed message. The first output transformed message is subjected to a second input transformation to produce a second input transformed message. The second input transformed message is processed by a second iteration of the CMEA process using the second CMEA key to produce a second intermediate cipher text. The second intermediate cipher text is

subjected to a second output transformation to produce a second output transformed message. According to another aspect of the present invention, the first and second iterations of the CMEA process employ tbox functions with inputs permuted by secret offsets. According to another aspect of the present invention, the plaintext may be processed by first and second iterations of the CMEA process using first and second CMEA keys, without being subjected to input and output transformations. Encrypted text may be suitably decrypted by introducing cipher text and reversing in order and inverting the steps applied to encrypt plaintext.

Etzel does not explicitly disclose regarding defining keys (public and private) and message decryption utilizing quadratic equation.

However, Brands does disclose in column (7 lines 1-5) that the composite number n is a product of two distinct prime numbers p and q. The secret key is the prime factorization of n where the secret key is private key.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Etzel to include factorized private key for the advantage of providing greater protection against attacks on data transmission.

Etzel and Brands are cited the claim limitation above. However, the combination of Etzel and Brands fails to specifically disclose regarding elements of public key and message decryption utilizing quadratic equation.

However, Cocks does disclose in page (360 sections 2) that the system generates a universally available public modulus M. This modulus is a product of

two primes P and Q where the modulus M is a public key. Cocks does disclose in page (361 section 3 lines 7-32) that a is a square modulo both P and Q, and hence is a square modulo M, or else –a is a square modulo P, Q and hence M. either a or –a will be quadratic residues modulo P and Q where the authority can calculate the square root modulo M and send it to Alice. Alice decrypted message s by calculating Jacobi symbol to recover original message. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Etzel and Brands to include quadratic equation for message decryption for the advantage of preventing attacks by providing greater protection on encrypted data transmission.

4. Claims 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Etzel, Brands and Cocks further in view of Patera et al. (US Patent No. 6,792,108).

Regarding claim 18, Etzel does disclose in figure (3) and column (4 lines 60-66) that at step 306, the first input transformed message is subjected to a first iteration of a CMEA process using a first CMEA key to produce a first intermediate cipher text. Etzel does disclose in figure (3) and column (5 lines 9-15) that at step 312, the transformed intermediate cipher text is subjected to a second iteration of the CMEA process, using a second CMEA key to produce a second intermediate cipher text. The second iteration of the CMEA process

preferably employs the improved use of the tbox function described in our above mentioned application.

The combination of Etzel, Brands and Cocks does not explicitly disclose regarding message is made up of an N-tuple.

However, Patera does disclose in column (20 lines 4-10) that the insertion of random bits into the encrypted message is done assuming that it is known which quasi-crystal points belong to the chosen subquasi-crystals. Then the n-tuples of bits corresponding to these quasi-crystals points in the encrypted message is known. Before transmitting any such n-tuple, j random bits are inserted where j value is added in each iteration steps.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Etzel, Brands and Cocks to include N-tuple message segments for the advantage of preventing attacks by providing greater protection on encrypted data transmission.

Regarding claim 19, Etzel does disclose in figure (3) and column (4 lines 60-66) that at step 306, the first input transformed message is subjected to a first iteration of a CMEA process using a first CMEA key to produce a first intermediate cipher text. Etzel does disclose in figure (3) and column (5 lines 9-15) that at step 312, the transformed intermediate cipher text is subjected to a second iteration of the CMEA process, using a second CMEA key to produce a second intermediate cipher text. The second iteration of the CMEA process

preferably employs the improved use of the tbox function described in our above mentioned application.

Cocks does disclose in page (361 lines 33-36) that if Bob does not know which of a or − a is the square for which Alice holds the root, he will have to replicate the above, using different randomly chosen t values to send the same x bits as before, and transmitting s = (t − a/t) mod M to Alice at each step. This doubles the amount of keying data that Bob sends where multiple values of a is resolved by transmitting additional data from Bob to Alice.

The combination of Etzel, Brands and Cocks does not explicitly disclose regarding adding bits in each iteration step.

However, Patera does disclose in column (20 lines 4-10) that the insertion of random bits into the encrypted message is done assuming that it is known which quasi-crystal points belong to the chosen subquasi-crystals. Then the n-tuples of bits corresponding to these quasi-crystals points in the encrypted message is known. Before transmitting any such n-tuple, j random bits are inserted where j value is added in each iteration steps.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Etzel, Brands and Cocks to include adding bits for the advantage of preventing attacks by providing greater protection on encrypted data transmission.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent No. 6,553,120, "Method for Data Decorrelation".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MORSHED MEHEDI whose telephone number is (571) 270-7640. The examiner can normally be reached on M - F, 8:00 am to 5:00 pm EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian T. Pendleton can be reach on (571) 272-7527. The fax number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from their Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (In USA or Canada) or 571-272-1000.

/ Morshed Mehedi/

Examiner, Art Unit 4124

/Brian T. Pendleton/

Supervisory Patent Examiner, Art Unit 2425